QUALIFIED TIME-STAMPING

1. OBJECT

The purpose of these conditions is to specify the modalities of request and use of qualified time-stamps proposed to subscribers, as well as the respective commitments and obligations of the related parties. The Terms and conditions arise from the Time-stamping Policy identified by the 1.2.250.1.177.2.9.1 OID available at the following address:
http://politique.certigna.fr/en/PHcertignaTSA.pdf.

2. DEFINITIONS

- **Subscriber** - Legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations.
- **Certification Authority** - In a Trust Service Provider (TSP), a Certification Authority is responsible, on behalf and under the responsibility of this TSP, applying at least one certification policy and is identified as such, as an issuer («issuer" field of the certificate).
- **Timestamping Authority (TSA)** - Authority responsible for the management of a timestamp service in compliance with Time-stamp Policy and relying on one or several TSU.
- **Electronic Seal** - Digital Seal done by an application server with data to be used either as part of an authentication service data origin, either as part of a service non-repudiation.
- **Electronic Certificate** - Electronic file certifying the link between a public key and the identity of its owner (natural or legal person or system). This certificate takes the form of an electronic signature made by a TSP. It is issued by a CA. The certificate is valid for a given period specified therein.
- **Time-stamp** – Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.
- Coordinated Universal Time (UTC) - Time scale based on the second as defined in Recommendation ITU-RTF.460-6.
- **Certificate revocation list (CRL)** - List including serial numbers of certificates that have been revoked, and signed by the issuing CA.
- **Time-stamp Policy (TP)** – Set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements.
- **Time-stamping service** - Trust service for issuing time-stamps.
- **Time-stamping Unit (TSU)** - Set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.
- **UTC(k)** - Time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.
- **Time-stamp user** – Entity (person or application) which relies on a time-stamp issued under the time-stamp Policy.
- **End user** – Subscriber or user of time-stamps.

3. AUTHORITY AND TSU CERTIFICATES

The “Certigna TSA” is a service of the DHIMYOTIS company localized in FRANCE. The TSU of the TSA use time-stamping seal certificates of the “Certigna Entity CA” certification authority. These certificates have got a name with the following syntax « DHIMYOTIS - TSU <N° de la TSU> ».

4. COMPLIANCE

Time-stamps are issued in compliance with the requirements of eIDAS Regulation (EU) N°910/2014 and the requirements of ETSI EN 319 421.

5. ACCURACY AND LIMIT OF USE

The TSU ensures that its clock is synchronized with UTC within an accuracy of one second.
Time-stamps can be verified at least 2 years after their generation.
Time-stamps issued are not kept and archived by the TSA.

6. DURATION

The contract is concluded for a period chosen by the Subscriber at the subscription to time-stamping service.

7. OBLIGATIONS OF SUBSCRIBER

The subscriber has the duty to issue a request using a hash algorithm supported by the TSA (SHA256, SHA384 or SHA512).
It is recommended that the subscriber, at the time of obtaining a time-stamp, verify that the certificate of the time-stamp unit is not revoked.

8. OBLIGATIONS OF USERS OF TIME-STAMPS

To trust a time-stamp, the users must:
- Verify that the time-stamp has been successfully signed, and that the certificate of the TSU is valid at the time of verification.
- Consider the limitations on the use of the time-stamp indicated in the TP and these Terms and Conditions.

9. OBLIGATIONS OF THE TSA

The TSA performs all or part of these functions directly or by subcontracting them. In any case, the TSA retains the responsibility. The TSA undertakes to comply with the obligations described in this Time-stamp Policy and ensures that these requirements are met. It also undertakes that the components of the TSA, internal or external to the TSA, to which they are applicable also respect them. The TSA:
- ensures the compliance with the requirements and procedures prescribed in this policy, even when the time-stamp features are implemented by subcontractors.
- adheres to any additional obligations indicated in the time-stamp either directly or incorporated by reference.
- provides time-stamping services in accordance with this TP and the associated TPS.
- fulfills all its commitments as stipulated in the Terms and Conditions.

10. CERTIFICATE STATUS CHECKING MEANS

To verify the certification chain, the subscribers and users can download the authority certificates (root CA and intermediate CA) and UH certificates from the website: https://www.certigna.fr.
To verify the revocation status of a certificate, the CA periodically publishes the CRL and offers an information service on the revocation status of the certificates (OCSP server, for On-line Certificate Status Protocol).
This list of revoked certificates and these services are accessible for applications using certificates at the addresses contained in the certificates:

To access the CRL :	To access the OCSP server:
http://crl.certigna.fr/entityca.crl	http://entityca.ocsp.certigna.fr
http://crl.dhimyotis.com/entityca.crl	http://entityca.ocsp.dhimyotis.com

11. LIMIT OF LIABILITY

The TSA may not be held liable for any unauthorized or improper use of time-stamps issued by its time-stamping service.
The TSA shall under no circumstances be held liable for any damage caused using the time-stamps issued by the TSA.
The TSA cannot be implicated by delays or losses that the transmitted data on which a time-stamp is requested by the application service.
The TSA cannot be held liable for problems related to force majeure, within the meaning of the Civil Code. If a case of force majeure has a duration exceeding fifteen days, the subscriber will be authorized to terminate the contract and there will be no prejudice.
The data transmitted in a time-stamp request and the verification of their value in the associated response remain the responsibility of the subscribers.

12. CONTRACT AND MODIFICATIONS

The contract cancels any previous commitment.
The subscriber agrees that during the term of the contract, the TSA may modify the Terms and conditions. However, the conditions accepted and signed by the subscriber remain valid throughout the duration of the contract unless the subscriber explicitly accepts the new conditions issued and published by the TSA on the website https://www.certigna.fr. In this case, a letter must be sent to the TSA together with the new Terms and conditions marked "read and approved", the date and signature of the subscriber. In the event of renewal of the contract, the time-stamps are subject to the applicable Terms and conditions.

13. TERMINATION

If one of the parties fails to fulfil one of the obligations arising from these Terms and conditions, the other party may notify him of the performance of the said obligation. Failing that for the defaulting party to have executed within fifteen days of such notification, the other party may terminate the contract.

14. CONDITIONS OF REFUND

Any time-stamp issued cannot be the subject of a refund request.

15. PRIVACY POLICY

Personal data will be used by the TSA only as part of the time-stamping services. The subscriber is informed that its personal identity information can be used as authentication data in the event of a request (e.g. renewal of contract). The TSA shall inform the subscriber that the certificate requests containing the personal data are archived at least seven years and as long as necessary for the purposes of providing proof in legal proceedings in accordance with applicable law. The information that any subscriber gives to the TSA is fully protected against disclosure and transfer to a third party without its consent or only in the context of a judicial decision or other legal authorization.

16. ASSIGNMENT OF THE CONTRACT

The subscriber cannot assign its rights to the contract.

17. DISPUTE RESOLUTION

The contract is subject to French law.
Parties undertake to try to resolve amicably any dispute which may arise between them, either directly or through a mediator, within 2 months of receipt of the letter with acknowledgment of receipt of the dispute. Half of the costs of mediation shall be borne by each of the parties. If necessary, the case will be brought before the Commercial Court of Lille.

18. DHIMYOTIS CONTACT INFORMATION

Dhimyotis S.A.
Zone de la plaine,
20 allée de la râperie 59650 Villeneuve d'Ascq, FRANCE
Phone : +33 320 792 409 - Fax : +33 956 952 412
Email : contact@dhimyotis.com